CYCRAFT

Crafting AI Agents for a Safer, Smarter World

CyCraft Product Catalog

Contents

Introduction 1

CyCraft Research 4

XecGuard 5

XecART 7

XCockpit 8

XCockpit: EASM 10

XCockpit: IASM 12

XCockpit: Endpoint 14

ThreatWall 16

SEMI E187 17

CyCraft Board Games 18

Crafting AI Agents for a Safer, Smarter World

In the post-AI era, cybersecurity has become an imperative that organizations and society cannot afford to ignore.

CyCraft (7823.TW) is a leading cybersecurity company dedicated to automating cybersecurity with AI technology. In 2017, CyCraft established the headquarter in Taiwan, with subsidiaries in Japan and Singapore. Based on the expertise in AI technology and the experience in handling cybersecurity incident investigations, CyCraft integrates AI and machine learning into defensive solutions. We continue delivering professional cybersecurity services to government agencies, financial sectors, and high-tech manufacturers worldwide.

CyCraft's product suite encompasses AI RedTeaming for automated validation of Large Language Model (LLM) security and strengthening cloud and on-premise AI models with AI Guardrail technology—aiming to build multi-layered cybersecurity resilience for the entire AI ecosystem. The XCockpit AI platform integrates three pillars of XASM (Extended Attack Surface Management): EASM, IASM, and Endpoint protection, providing enterprises with proactive, preventative, and real-time deep defense.

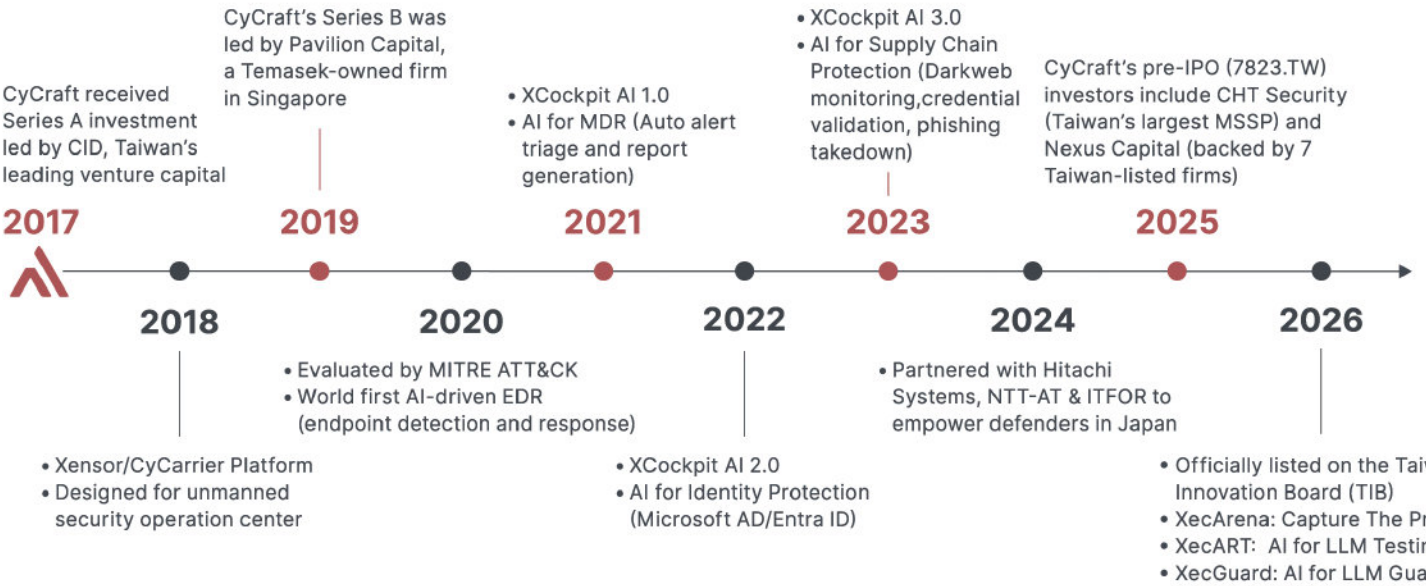
CyCraft's long-term collaboration with government, finance, high-tech semiconductor and other major industries continues to encourage us on safeguarding enterprise digital resilience. Since 2024, CyCraft has established international partnership in Japan, Korea, Malaysia and broader APAC area. Officially listed on the Taiwan Innovation Board (TIB) in 2026, CyCraft is devoted to bring Taiwan expertise onto global stage.

CyCraft firmly believes that cybersecurity is the cornerstone supporting social stability and development, and AI technology is the key to fortifying its future. Driven by the mission to "Empower Enterprise Cybersecurity with Innovative AI Technology," CyCraft has received multiple recognitions from leading research organizations such as Gartner, IDC, and Frost & Sullivan, along with numerous awards locally and internationally. As a member of multinational cybersecurity organizations, CyCraft continues to advance global cybersecurity development.

President Lai Ching-Te Visits CyCraft at 2025 CyberSec

President Tsai Ing-Wen Awards CyCraft with 2023 NEXT BIG Startup Initiative

Cybersecurity Starts with CyCraft



Our Service at Scale

600,000 endpoints. 1 PB of traffic. 300 million threat signals - every single day.

Government & CI	Financial Services	Semicon & Defense
100+	100+	100+
Priority: Regulation	Priority: Reliability	Priority: Resilience

International Partnership

ACT アクト
DDS DIGITAL DATA SOLUTION INC.
ENZOPLUS
FUTURE SECURE WAVE
株式会社 日立システムズ
INFOSEC
ITFOR
MACHINA RECORD
Mitsubishi Research Institute
NTT AT NTTアドバンステクノロジ株式会社
NTT Security
SECTONICS
Secure Innovation
Smartnet CONNECTING SUCCESS
TOSHO COMPUTER SYSTEMS Co.,Ltd

Awards and Recognitions

Interop BEST 2020
CYBER SECURITY EXCELLENCE AWARDS WINNER 2020
CYBER SECURITY EXCELLENCE AWARDS WINNER 2021
CYBER SECURITY EXCELLENCE AWARDS WINNER 2022
FROST & SULLIVAN INSTITUTE ENLIGHTENED GROWTH LEADERSHIP EMERGING COMPANIES, 2023
HR Asia BEST COMPANIES TO WORK FOR IN ASIA 2023

CyCraft XASM AI: Core Products & Services

Endpoint Agent

EDR / MDR - Advanced threat detection and esponse with AI-powered EDR deployed on 500K+ sensors worldwide, providing real-time protection against zero-day exploits and sophisticated malware.

Exposure Agent

EASM - External attack surface monitoring discovering vulnerabilities across internet- facing assets, cloud infrastructure, and dark web before attackers can exploit them.

Identity Agent

IASM - Identity - Active Directory and Entra ID privilege analysis with attack path detection, identifying privilege escalation vulnerabilities before attackers exploit them.

CyCraft Research

10+ international research papers published annually at top conferences including NeurIPS, EMNLP, advancing the state of AI-powered security defense.

XCOCKPIT
CyCraft AI Copilot

500K+ AI security sensors

deployed worldwide, providing continuous threat intelligence and real-time protection across diverse enterprise environments.

Assessment and Compliance

SEMI E187 - Automated compliance assessment for semiconductor manufacturing and critical infrastructure equipment with minimal manual effort.

TIG Gateway

ThreatWall - Network threat gateway providing real-time traffic inspection, and automated threat blocking at the network perimeter to prevent lateral movement.

AI Model Guardrail

XecGuard - LLM Guardrail - Advanced protection against prompt injection, model manipulation attacks, and data exfiltration through large language models.

Pioneering R&D Performance Aligned with Gartner's Emerging Tech Insights

Gartner

Emerging Tech: Unified Exposure Management Will Drive Displacement of Fragmented Point Solutions

29 September 2025 - ID G00810698 - 15 min read

By: Luis Castillo, David Senf, Tom Powledge

Initiatives: Emerging Technologies and Trends Impact on Products and Services

> Fragmented exposure management point solutions can't handle today's complex, integrated environments, leading to blind spots, siloed workflows, slow responses, and high risk. Product leaders must refocus priorities to overcome fragmentation from disparate tools and operationalize the CTEM life cycle.

Sample Vendors: [redacted] *CyCraft Technology,* [redacted]

Gartner

Emerging Tech Impact Radar: Preemptive Cybersecurity

7 October 2025 - ID G00830315 - 46 min read

By: Emerging Tech and Trends Security Research Team

Initiatives: Emerging Technologies and Trends Impact on Products and Services

> Traditional cybersecurity based on a reactive detection and response approach is struggling against emerging AI threats and failing to keep pace in many cases. C-level executives must embrace a new preemptive strategy to neutralize threats before they can cause harm.

Sample Vendors

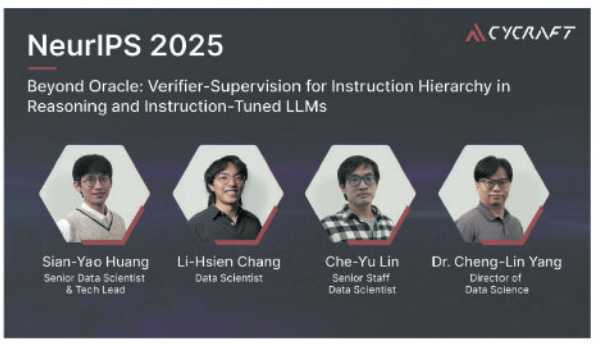
[redacted] CyCraft, [redacted]

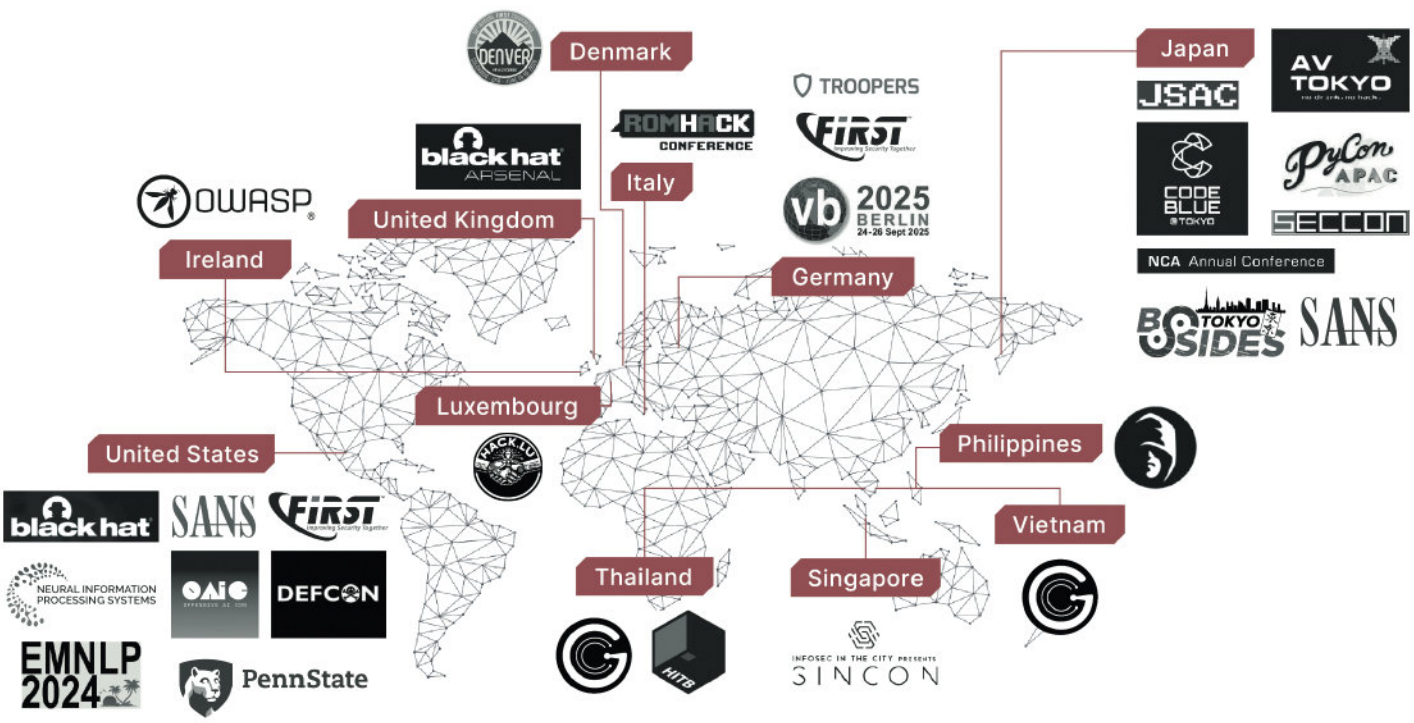
CyCraft Research

CyCraft research momentum embodies the principle: "Taiwan's Hacker Spirit + Practical Experience against Threat Actor = Frontline Cyber Warfare Capability." From tracking APT attacks and monitoring dark web intelligence to establishing threat exposure management platforms and developing the AI-powered XecGuard application, CyCraft stays ahead of emerging trends and pioneers the future of cybersecurity. Beyond continuously publishing frontier research at international conferences such as EMNLP, NeurIPS, BlackHat USA, FIRST CON, and TROOPERS, we also take pride in cultivating the next generation of cybersecurity professionals.

NeurIPS 2025

Current LLMs frequently encounter authority hierarchy confusion when processing multi-level directives. In response, CyCraft research team has proposed an innovative "unified supervision framework" that embeds verifiable checkers into synthesized instruction-conflict instances, enabling self-supervised learning without requiring oracle labels or reasoning traces. On NeurIPS, CyCraft researchers demonstrated how this framework not only applies to different models but also significantly enhances both safety robustness and instruction adherence, pioneering the new research directions in AI information security.

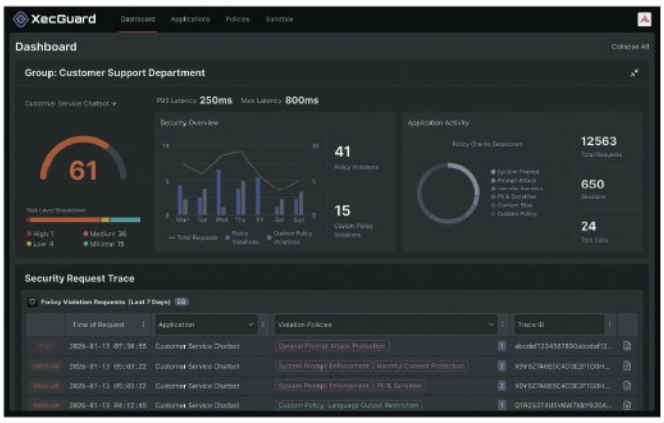




2025

NeurIPS—Beyond Oracle: Verifier-Supervision for Instruction Hierarchy in Reasoning and Instruction-Tuned LLMs
Offensive AI Con—WOOF! Sniffer Dog Off the Leash: Automating Active Directory Attacks with MCP
RomHack—Sign Here to Bypass: From macOS Intune PRT Cookie Theft to Entra ID Persistence
VB2025 Berlin—The silent infiltration: darknet analysis of corporate data exposures in East Asia
DEF CON 33—Original Sin of SSO: macOS PRT Cookie Theft & Entra ID Persistence via Device Forgery
Black Hat USA—All Talk, AI Action: Binary Analysis Toolkit MCP Server
Black Hat USA—Pay Attention to the Clue: Clue-Driven Reverse Engineering by LLM in Real-World Malware Analysis
TROOPERS—Breaking Down macOS Intune SSO: PRT Cookie Token Theft and Platform Comparison
First Conference—Aztronomy: Establishing the Foundation of Attack Path Analysis in Azure
First Conference—Breaking Down Barriers: Analyzing Active Directory Security Across Industries
SINCON—DarkMesh: A Knowledge Graph-Enhanced Blue Team Monitoring Tool for Telegram
SECCON 13—Temporal Forensics: Harnessing AI for Accurate Timeframes in Multilingual Cybersecurity Reports
SECCON 13—YaDa - Reverse Engineering with Yara Bytecode

Build AI fast. Keep it Safe.



AI Security Platform:
Visibility, Security and Auditability

XecGuard is CyCraft's AI Security Platform, integrating cybersecurity, compliance and ethics Guardrails. Covering Prompt management, governance and auditability, XecGuard supports diverse use scenarios across the entire application lifecycle.

What can XecGuard do for you?

Zero-Code AI Security

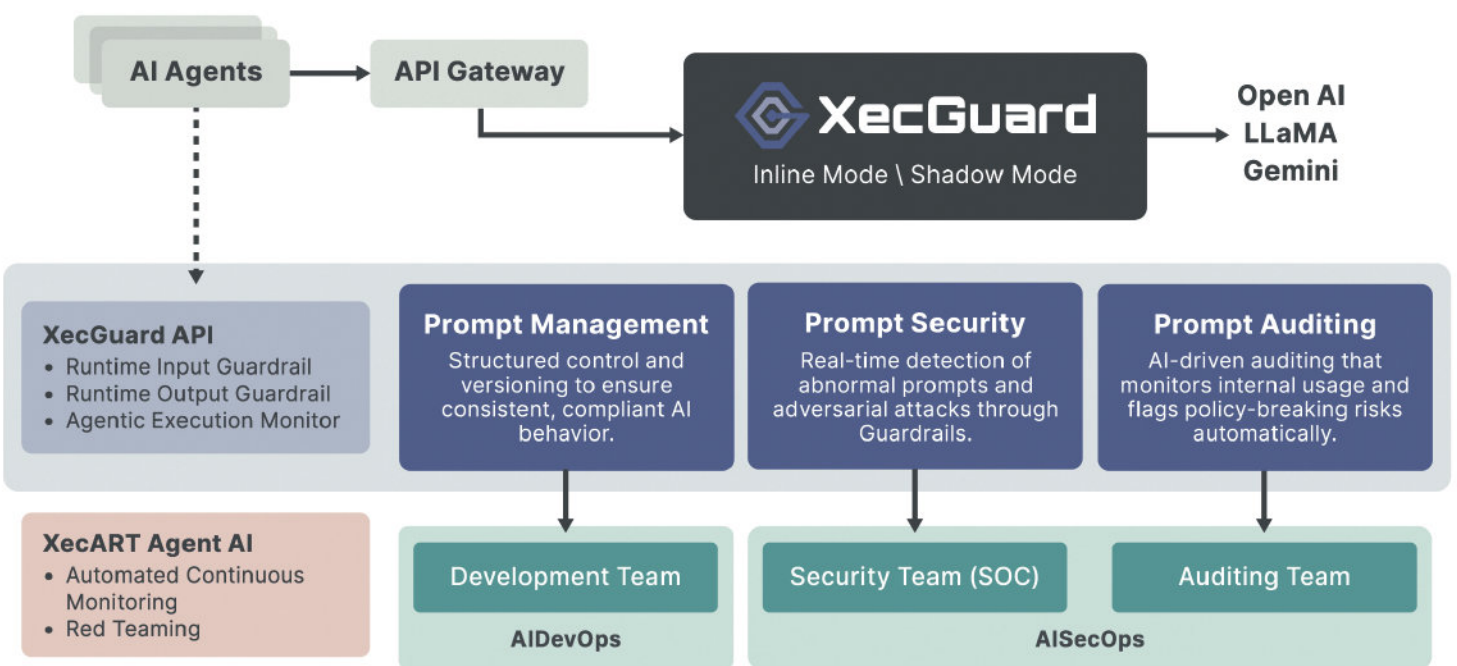
Enable enterprise-grade protection via an OpenAI-compatible API—no code changes required. Instantly defend against Prompt Injection and PII leakage.

Flexible Enterprise Guardrails

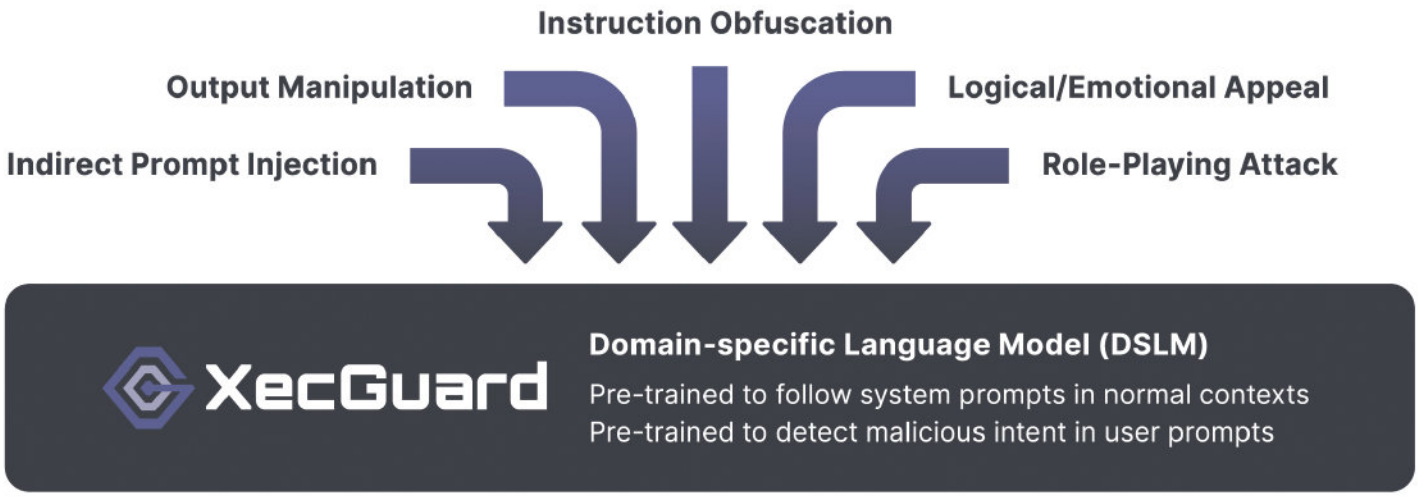
Supports Inline and Shadow modes with Prompt & Response Guardrails to detect and block risky interactions in real time.

Scalable AI Governance

Built for scale with auto-scaling, multi-tenant management, and seamless SIEM/SOC integration via Alert APIs.



XecGuard Prompt Governance



Prompt Injection

Causes the output to violate the system prompt (pre-defined rule)

Prompt Extraction

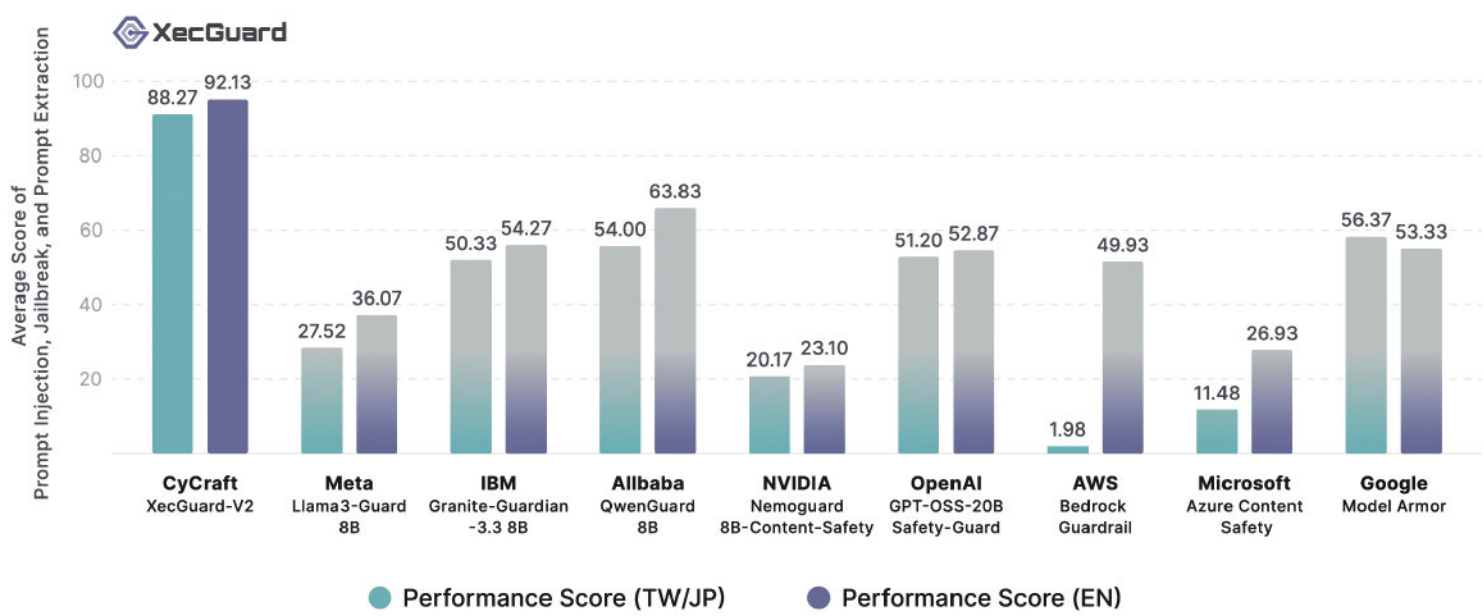
Causes the output to leak the system prompt (app configuration)

Jailbreak

Causes outputs that disobey the ethical values learned by the LLM

XecGuard not only covers traditional harmful content detection (Toxic, Harmful Content) but also integrates advanced context-aware instruction-following capabilities. It can interpret the application-specific rules defined in the System Prompt, intelligently identify attempts to bypass or violate those rules, and defend against a wide range of prompt injection attacks—providing real, effective protection for AI chatbot applications.

XecGuard Comparison with Other Models



In LLM Red Teaming assessments, XecGuard consistently outperforms other open-source Guardrail models. By leveraging its stronger System Prompt instruction-following ability, XecGuard enables LLMs to effectively resist various Prompt Injection contexts that violate System Prompts.

Hands-on Experience in Critical Domains

Built on CyCraft's Red Teaming and Blue Teaming experience across government, finance, and high-tech manufacturing, XecGuard goes beyond model-level defenses. It also delivers a deep understanding of attack scenarios and risk response strategies, ensuring that as enterprises rapidly adopt AI, they can simultaneously achieve information security, regulatory compliance and system resilience. XecGuard helps enterprises unlock the full value of AI, and at the same time, stay resilient against real-world threats.

Government

Financial

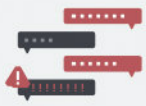
Semiconductor

Medical

Retail

XecART

Proprietary Red Teaming for Your AI DevOps



TESTING

AI Model Security Testing

Conduct multi-round dialogue testing of AI Chatbots to validate performance under diverse attack scenarios and assess defenses against prompt injection.

ASSESSMENT

AI Safety Compliance Assessment

Provide AI safety compliance reports aligned with OWASP, ISO, NIST, and regulatory guidelines to adhere to international standards.

EVALUATION

AI System Resilience Evaluation

Present multi-dimensional resilience assessment of AI systems, including external resilience, identity resilience, and anomaly response capabilities, to comprehensively enhance defense effectiveness.

Chatbot Security Assessment

CyCraft AI RedTeam

API Online Testing

Customized LLMs (Finetuned)
Chatbot System Prompt

AI Safety Compliance Mapping

- **Prompt Instruction Violation Testing**
  Prompt Injection / Indirect Prompt Injection / Sensitive Data Leak
- **Prompt Leakage Testing**
  Prompt Disclosure
- **Model Bias and Hallucination Testing**
  Content Bias / Hallucinations / Input Leakage
- **Public Moral or Ethical Standard Violation Testing**
  Unsafe Outputs / Toxic Outputs

CyCraft AI Copilot

Following the Continuous Threat Exposure Management (CTEM) framework, XCockpit focuses on enterprises' attack surface management to anticipate potential threats and exposures in advance. This AI-driven platform integrates three modules: External Attack Surface Management (EASM), Internal Attack Surface Management (IASM) and Endpoint Security Posture Management.

Risk Identification And Team Performance Metrics

Overall risk assessment and cybersecurity service team performance metrics (MTTI/MTTD)

AI-powered Virtual Analyst

Integrate AI automated analysis, incident explanation, decrease the cost of labor force, increase the efficiency

01 02 03 04

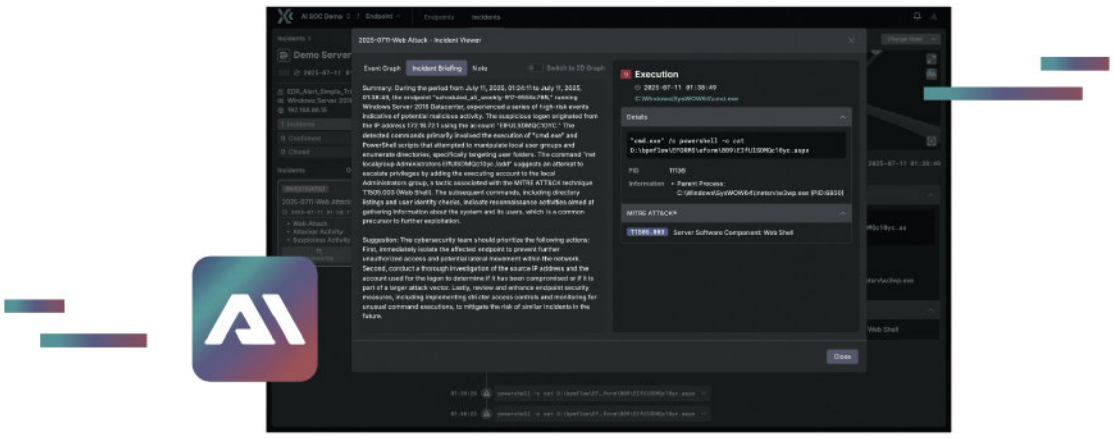
Comprehensive Threat Monitoring

EDR endpoint threat monitor + AD account monitor + ASM exposure

Visualized Cybersecurity Dashboard

Fast and simple interface, various operational report , incident real-time analysis and correlation analysis report

CyCraftGPT: Autonomous Incident Briefing

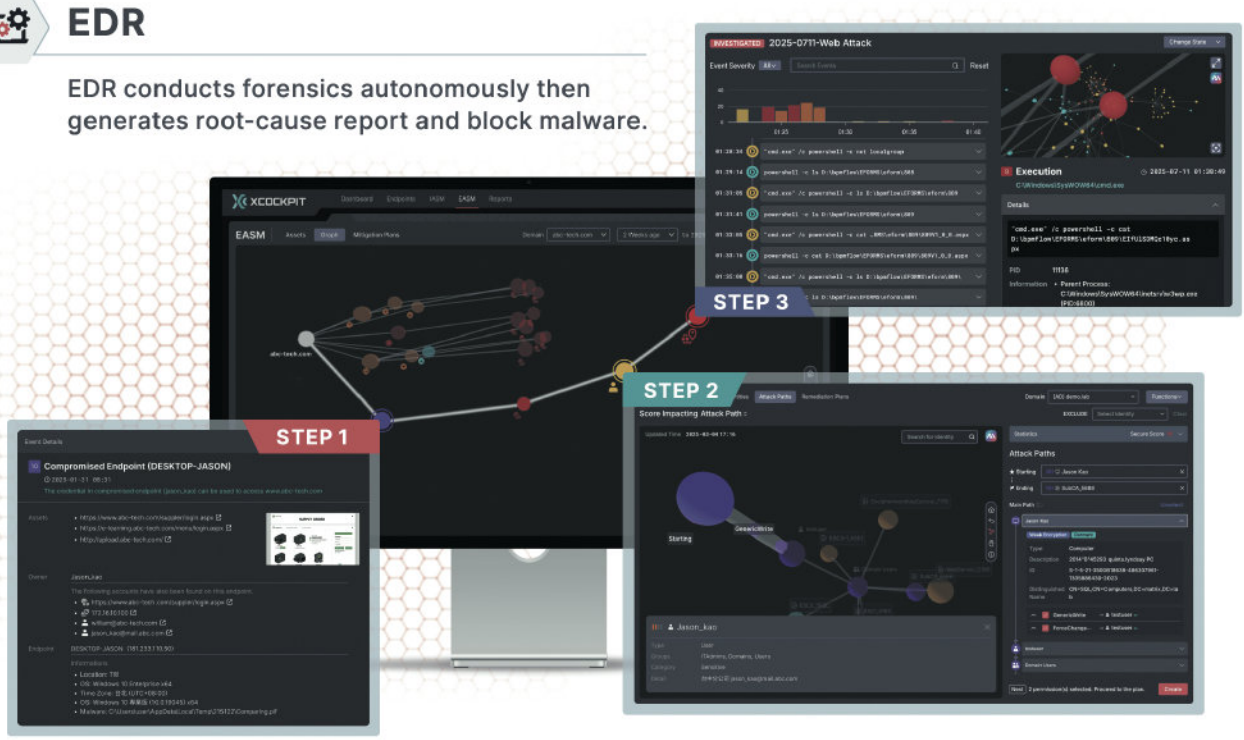


CyCraft's exclusively trained CyCraftGPT integrates domain expertise, case analysis, and explanatory capabilities in the cybersecurity field, addressing labor shortages and enhancing operational efficiency.

What can XCockpit do for you?

EDR

EDR conducts forensics autonomously then generates root-cause report and block malware.



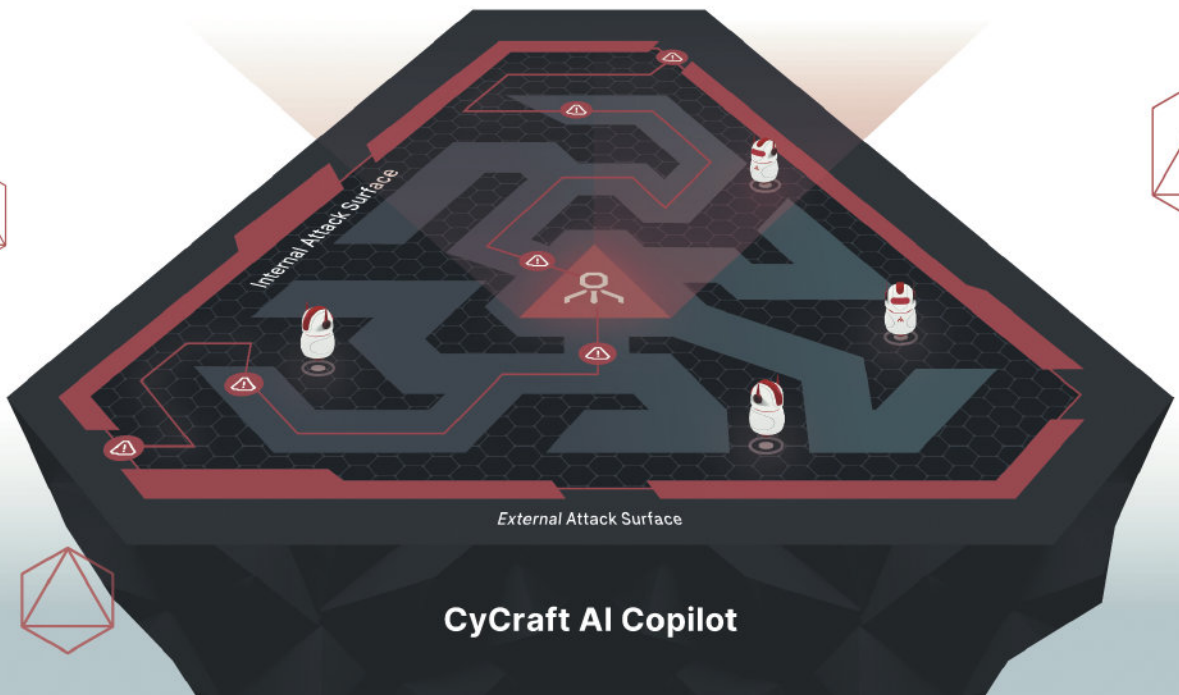
EASM

EASM identifies compromised work endpoint from darknet, (DESKTOP-JASON), Jason Kao.

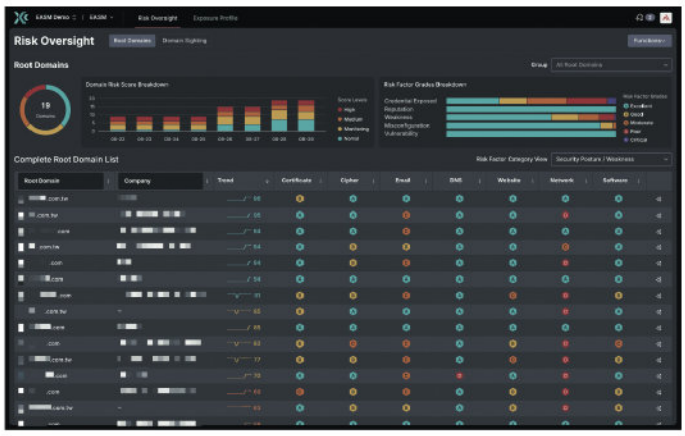
IASM

IASM analyzes attack paths in AD then identifies risk of compromised credential of supplier.

EASM	IASM	ENDPOINT
External Attack Surface Management	Internal Attack Surface Management	Endpoint Security Posture Management
Preemptive	Proactive	Preventive



CyCraft AI Copilot



Preemptive External Attack Surface Management

XCockpit EASM automatically discovers potential external attack surfaces and provides a comprehensive view of digital assets from the hacker's perspective. EASM also proactively identifies potential vulnerabilities through in-depth identification and analyzes the comprehensive security posture, correlating the attack surface of accounts, endpoints, and services.

AI-generated Compliance Assessment

An exclusively trained AI model offers practical audit recommendations and risk control measures, tailored to various cybersecurity management systems and regulatory requirements.

Early Warnings and Leakage Tracing

Leverage AI to inventory legitimate corporate credentials on the surface web, dark web, or public marketplaces, offering real-time alerts and mitigating attacks beforehand.

Continuous Exposure Management

Provide enterprises with intelligence of external assets, manage critical risks through case management, and continuously keep track of diachronic improvement performance.

What can EASM do for you?

01

Aligning with International Standards: NIST SP 800-30

XCockpit EASM and IASM solutions provide comprehensive support for visualizing, quantifying, and strengthening cyber threat management. They are both highly compatible with large-scale and complex organizational risk assessment frameworks such as NIST SP 800-30, enabling strategic security management.

02

Safeguarding Your Supply Chain Security

XCockpit EASM enables enterprises to discover exploitable vulnerabilities and manage exposed digital assets across their entire attack surface. By inventorying, monitoring, and responding to threats across both internal systems and subsidiaries, EASM fortifies your supply chain security.

EASM Service Procedure

Discovery > Assessment > Remediation > Reporting

Discovery
Identify, discover, and list digital assets like domains, IP addresses, and accounts.

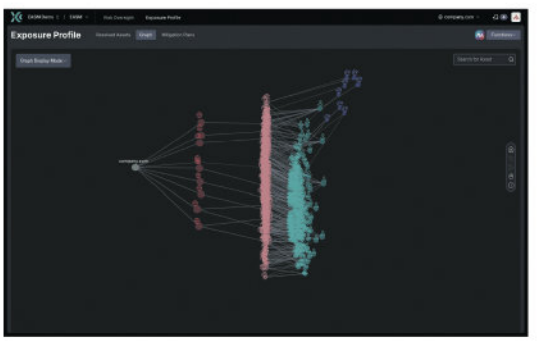
Assessment
Categorize and prioritize exposures based on severity, with AI-generated threat summaries and visualized event correlations.

Remediation
Automatically merge high-severity incidents into tickets and provide mitigation recommendations.

Reporting
Provide the security overview with status reports on asset classification, incident categories, and ticket resolutions.

Visibility Fosters Efficiency

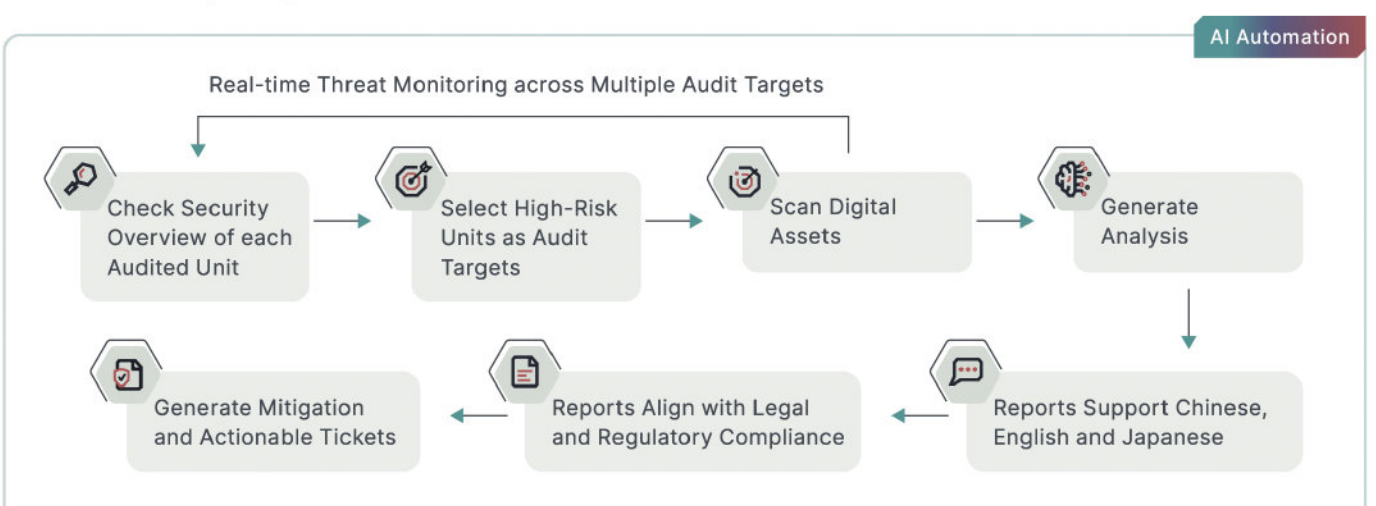
EASM visualizes external exposure correlations, displaying them by risk level and digital asset categories. This instant visibility into all risks across organizations fosters proactive efficiency.

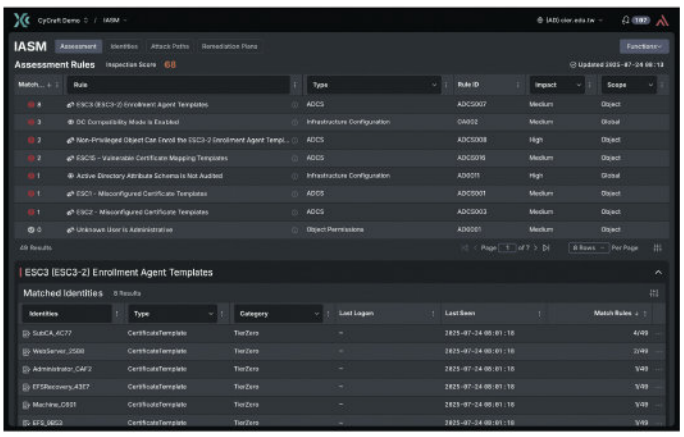


XCOCKPIT EASM USE CASE

Government Scenario: Streamlining Audit Operations

The government agency needs to conduct annual audits across a wide range of government-affiliated organizations, including public agencies, government-funded foundations, state-owned enterprises, and critical infrastructure operators.
Instead of traditional questionnaire-based methods, **XCockpit EASM** optimizes audit process and provides highly reliable data. This efficient and objective approach enhances audit responsiveness across multiple organizations.





Proactive Internal Attack Surface Management

XCockpit IASM provides visibility into the hidden relationships of all assets, services, endpoints, groups, and accounts, whether stored on-premises or in the cloud, revealing key identity exposures and supplying quantitative threat indicators. By continuously monitoring privileged accounts, detecting AD attacks, and integrating threat situational awareness data, IASM proactively controls your internal attack surfaces.

Account Impact Analysis

Use AI to simulate account impact analysis, anticipate hackers' attack paths, and discern the enterprise's privilege perimeters.

Monitor for Warning Signs

Monitor abnormal privileged account activity, detect common AD account attack methods in real time, and identify any signs of an attack.

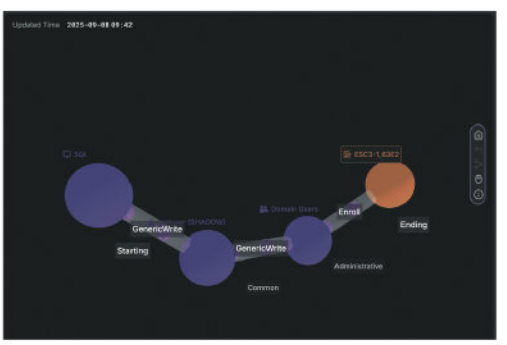
Quantitative Identity Management

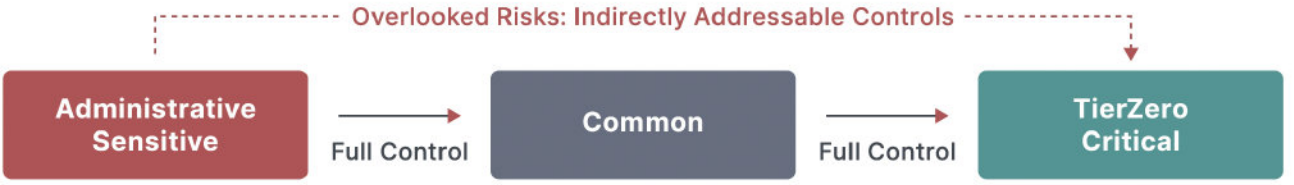
Stay in control of identity attack surfaces, quantify the enterprise's identity security indicators, and obtain an overall security posture.

What can IASM do for you?

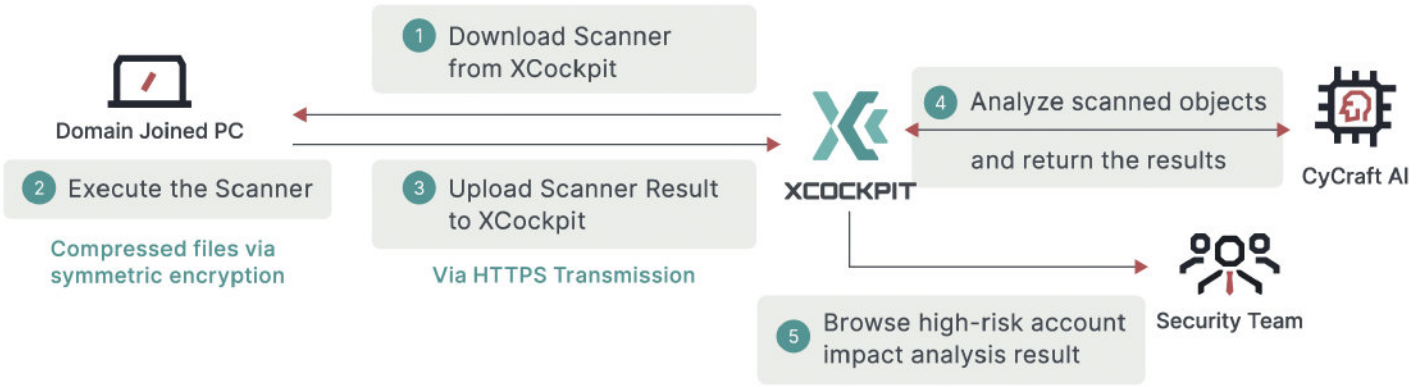
Uncovering Attack Path and Misconfiguration

Permission misconfigurations between AD objects can let low-privileged (Administrative/Sensitive) objects indirectly control high-privileged objects (Tier Zero/Critical). IASM uncovers attack paths hidden in complex configurations.

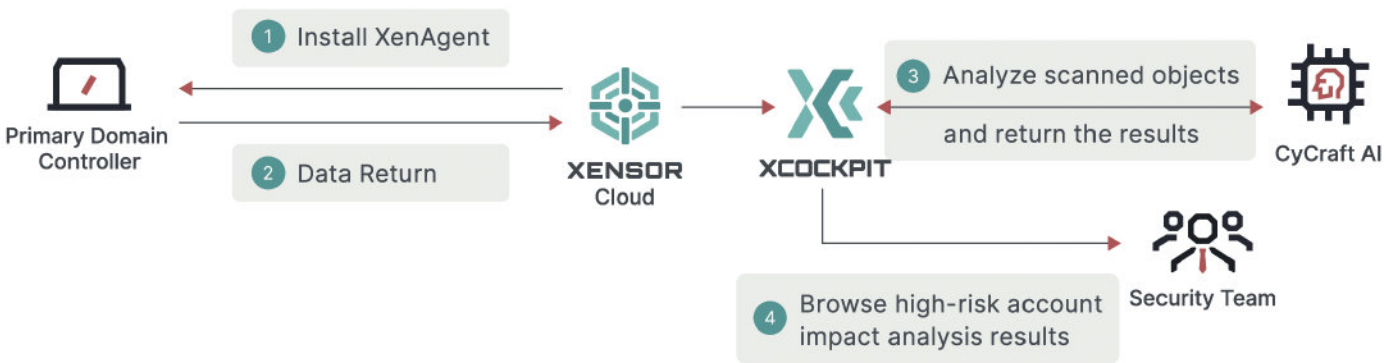




AD Insight Offline Scan

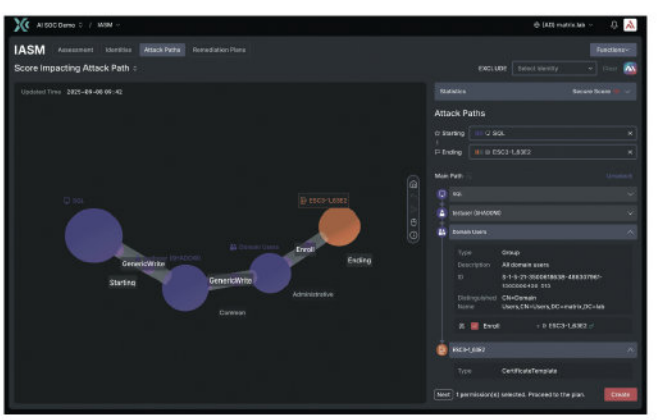


MDR Agent Real-time Monitoring



Unveiling AD Risks with Attack Path Simulation

IASM simulates possible attack paths, identifies potential privileged accounts, and implements mitigations. Over 40% of recent unauthorized intrusions are due to spoofing using legitimate user accounts and passwords, according to a global cybersecurity vendor. Start unveiling your AD risks with IASM as a first step for Identity management.

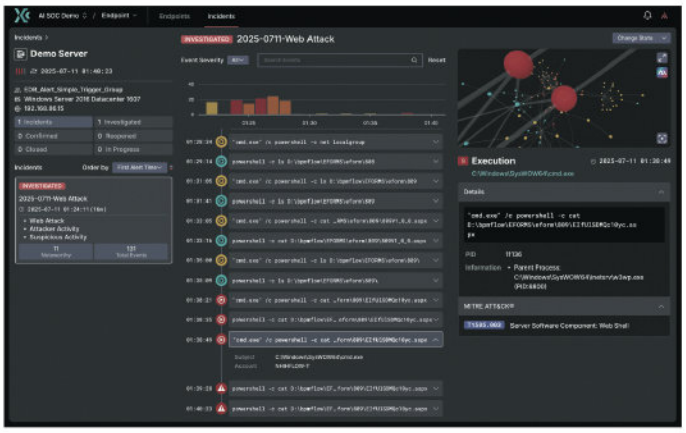


XCOCKPIT IASM USE CASE

Online Payment Company in APAC: Inventorying Identity Posture

This APAC-based online payment company requires a complete Identity security assessment on existing Active Directory Platform. Instead of manual investigation by analysts, the company pursues tools that are more convincing and efficient.

By adopting XCockpit IASM, the company achieved faster and more accurate Identity risk analysis. IASM not only supports AI-generated incident briefing and remediation plans, but also complies to Technology Risk Management (TRM) under Security Commission of the company.



Profound Endpoint Security Posture Management

XCockpit Endpoint monitors activities 24/7, detects prevalent hacker attack techniques in real time, and identifies any signs of an attack. By managing everything from ticket creation to closure, XCockpit Endpoint allows IT administrators to focus on handling pending tickets with automated workflow.

Autonomous Cybersecurity Response

Analysis based on the context of the case and autonomous case management increases the productivity of your cybersecurity team and enhances cyber resilience.

Enhanced Team Efficiency

Innovative AI language model trained for use in cybersecurity scenarios that can automatically summarize attack incidents and collaborate closely with the team, thereby solving workforce shortages.

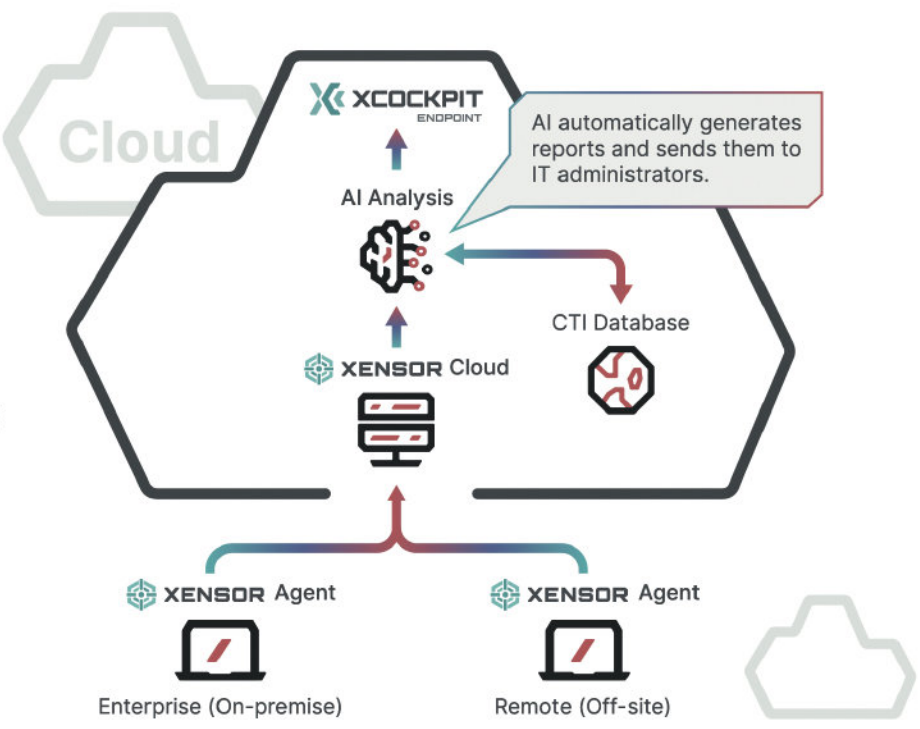
Quantitative Endpoint Management

24/7 threat hunting with automatically ticket creation and investigation, all with MTTI (Mean Time To Investigate) and MTTD (Mean Time To Detect) data provided.

Endpoint Service Procedure

01 Install the agent, data analysis and incident management are entirely conducted on CyCraft's cloud, with no additional assets requried than a browser.

02 AI-generated analysis reports prioritize high-priority issues first, ensuring efficient operations.



XCOCKPIT ENDPOINT USE CASE

High-Tech Manufacturing: Full-Spectrum Defense Following Threat Exposure

A prominent Taiwanese LCD backlight module manufacturer faced an advanced attack after its identity and access management system was compromised and subjected to privilege escalation. Having historically deployed only traditional endpoint protection, the company struggled to defend against Identity-based attacks. Consequently, they required a solution to rapidly intercept post-compromise lateral movement, halt threat expansion, and comprehensively deploy both Endpoint and real-time Identity management systems.

XCockpit Endpoint assisted in providing 24/7 monitoring across more than 5,000 endpoints and servers, leveraging AI technology to detect and successfully block hackers from launching attacks via Active Directory (AD) privilege escalation. Furthermore, Endpoint swiftly clarified the root cause of the incident and identified potential vulnerabilities, effectively transforming the company's cybersecurity posture from passive patching to proactive defense.

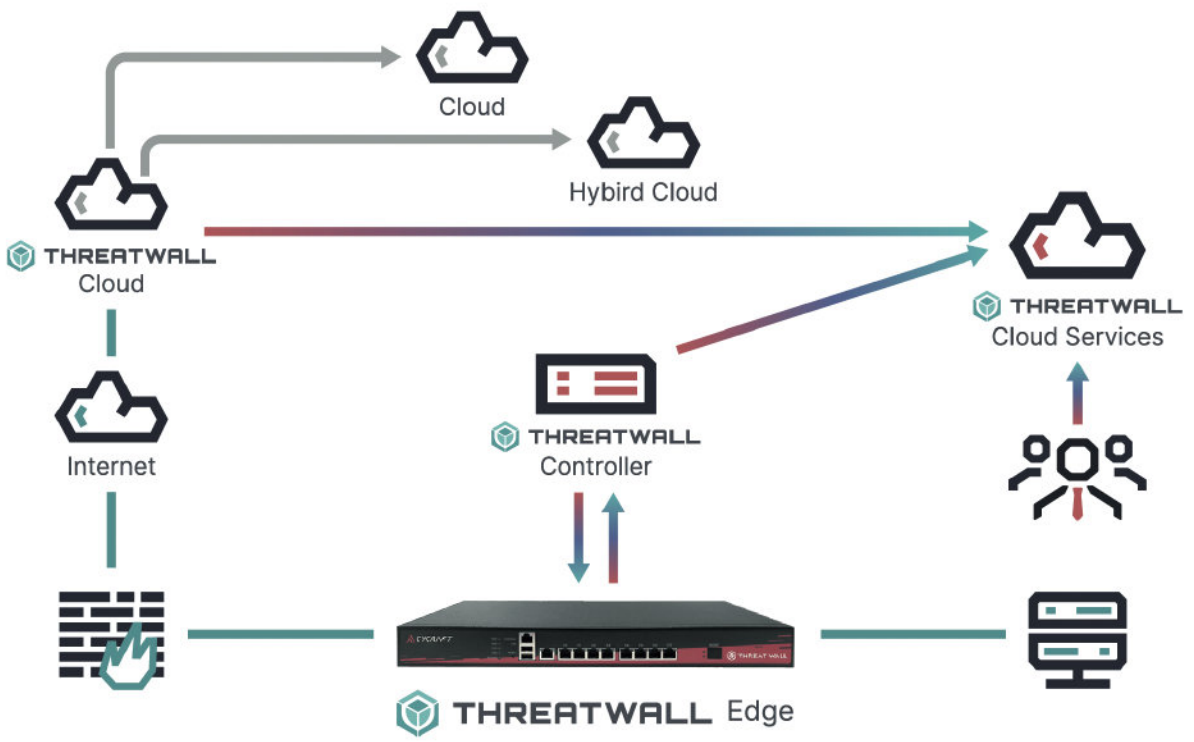
Jamf x CyCraft

CyCraft XCockpit integrates Jamf Pro and Jamf Protect, providing visualized, autonomous detection and quantifiable security metrics against emerging threats. The XCockpit platform is also aligned with Gartner's Unified Exposure Management (UEM) solution. The collaboration between Jamf and CyCraft comprehensively protects Apple devices, macOS/iOS systems and organizational threats.

ThreatWall

Real-Time Threat Intelligence Gateway

ThreatWall Threat Intelligence Gateway (TIG) unifies automated detection and response with the latest global threat intelligence surveillance in one multi-purpose box that stands guard 24/7/365. ThreatWall blocks both potential inbound threats from entering and compromising your environment as well as outbound traffic towards any unauthorized or malicious C2 server.



Built-in Compliance Reports

Generate compliance reports that adhere to standards issued by various National Information Security Information Sharing and Analysis Centers (ISAC) and other institutions (including F-ISAC, etc.)

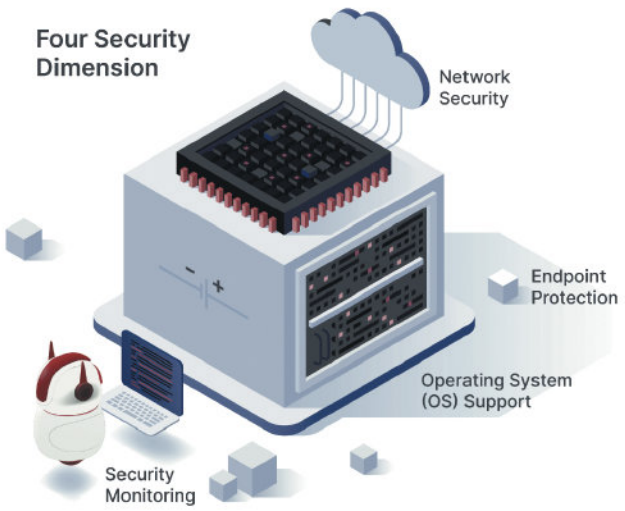
Blazingly Fast, Gloriously Global

ThreatWall enriches IOCs with up-to-date global cyber threat intelligence. Combined with AI-driven analysis, ThreatWall provides enriched and contextual threat intel on blacklists and malicious behavior.

Proactive Defense + Flexible Deployment

Gain up-to-date intel on malicious domains, C2 servers, IP addresses. Enjoy an IoC Capacity of over 50 million, and reduce the risk of zero-day attacks.

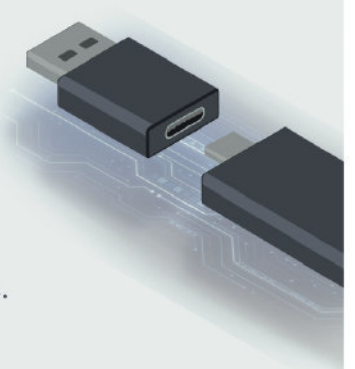
SEMI E187 Assessment Tool



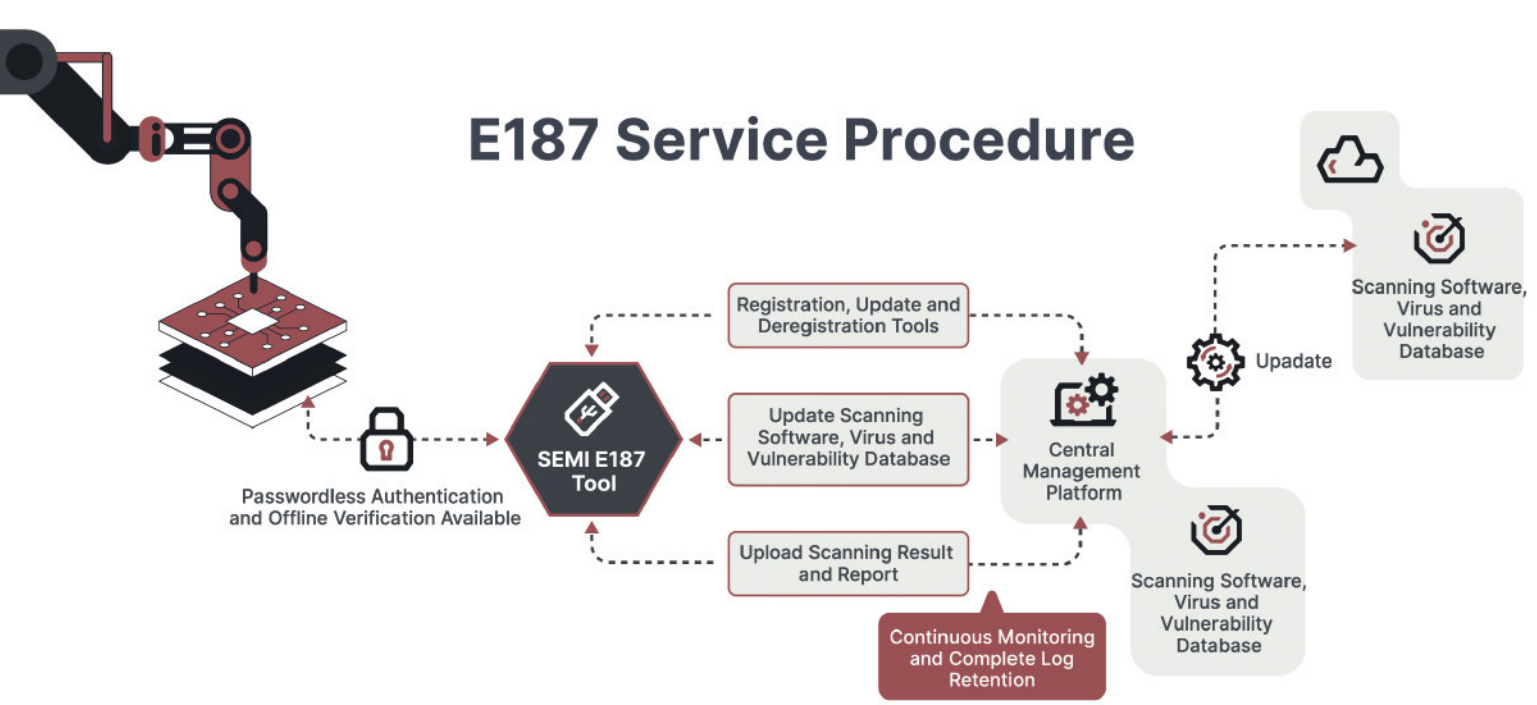
SEMI E187, the standard cybersecurity regulations, aims to efficiently decrease cybersecurity risks and to provide actionable guidelines for the entire semiconductor industry. SEMI E187 focuses on four security dimensions: operating system (OS) support, network security, endpoint protection, and security monitoring. By adhering to these guidelines, semiconductor manufacturers can safeguard their production lines, minimize downtime, and mitigate the potentially devastating impact of cyber threats.

The All-in-One SEMI E187 Tool

- Conduct comprehensive assessment through a single tool and ensure compliance with SEMI E187 standards.
- Available in Chinese, English, and Japanese interfaces.
- Perform instant scanning and generate detailed reports with a single click.
- Produce in-depth and concise reports in encrypted USB drives to ensure data integrity.
- Support offline scanning and detection.
- Customizable to scan and verify specific files, directories, or selected items.
- Incorporate FIDO2 authentication to enhance security.



E187 Service Procedure



“ Let’s Begin the Cybersecurity Journey ” with Board Games!

Struggling with complex cybersecurity knowledge? Lacking learning materials?
CyCraft self-develops these board games: Cybercan and Cybercrete.
Embedded with real security thinking, they help you to put theory into practice.

Cybercans

Understanding You Cybersecurity Posture

Cybercans incorporates the **Cyber Defense Matrix (CDM)** framework, mapping common attack and defense techniques, security incidents, and key concepts.

Cybercans Takeaways

- Asset types and corresponding defenses.
- Roles of security solutions across the attack lifecycle.
- Decision-making strategies within limited resources.
- Importance of resilience in security strategy.

Cybercrete

The Road to Security

Cybercrete is centered around **Continuous Threat Exposure Management (CTEM)** framework. Players, taking roles of an enterprise’s security team, need to cooperate and carry out CTEM strategies.

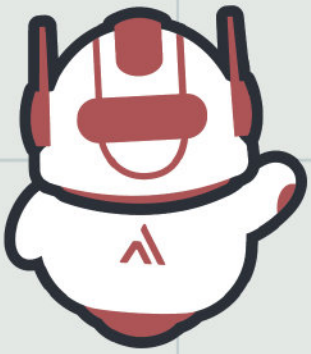
Cybercrete Takeaways

- Identify key roles and assets.
- Prioritize actions from both hacker and defender perspectives.
- Promote collaboration by taking different roles.
- Leverage intelligence in strengthening cyber defense.

Play the games, plan your defense

For enterprises, teams, educators and anyone who wants to learn cybersecurity through real-world simulation, please contact our local team for further information.

Notes



Crafting AI Agents for a Safer
Smarter World


CYCRAFT